Theoretical Computer Science 143 (1995) 149–158

Note

Weak completeness in E and E_2 ☆

David W. Juedes[1], Jack H. Lutz*

Department of Computer Science, Iowa State University, Ames, IA 50011, USA

Received March 1994; revised August 1994
Communicated by J. Diaz

Abstract

The notions of weak $\leqslant_m^P$-completeness for the complexity classes $E = DTIME(2^{linear})$ and $E_2 = DTIME(2^{polynomial})$ are compared. An element C of one of these classes is *weakly* $\leqslant_m^P$-*complete* for the class if the set $P_m(C)$, consisting of all languages $A \leqslant_m^P C$, does not have measure 0 in the class. The following two results are proven.

(i) Every problem that is weakly $\leqslant_m^P$-complete for E is weakly $\leqslant_m^P$-complete for E_2.
(ii) There is a problem in E that is weakly $\leqslant_m^P$-complete for E_2, but not for E.

1. Introduction

The completeness phenomenon is, to date, our principal tool for ascertaining the complexities of seemingly intractable computational problems. Problems that are complete for NP, PSPACE, or classes in between are *presumably intractable* because we are inclined to believe that $P \neq NP$. Problems that are complete for exponential time are *provably intractable* by the time hierarchy theorem of Hartmanis and Stearns [3]. In fact, such problems are now known to have very strong intractability properties [2, 4, 8, 15, 20, etc.].

Recently, Juedes and Lutz [7] initiated investigation of a measure-theoretic generalization of the completeness phenomenon in the exponential time complexity classes $E = DTIME(2^{linear})$ and $E_2 = DTIME(2^{polynomial})$. Specifically, a language (i.e., decision problem) C in one of these classes is defined to be *weakly* $\leqslant_m^P$-*complete* for the class if the $P_m(C)$, consisting of all languages $A \leqslant_m^P C$, does not have measure 0 in the

☆ This work was supported in part by National Science Foundation Grant CCR-9157382, with matching funds from Rockwell International, Microware Systems Corporation, and Amoco Foundation.
*Corresponding author. Email: lutz@cs.iastate.edu.
[1]Author's present address: Department of Computer Science, Ohio University, Morton Hall 416, Athens, OH 45701, USA.

SSDI 0304-3975(94)00232-0

class. ("Measure" here refers to resource-bounded measure, as developed by Lutz [9, 12]. Necessary details appear in Section 3.) Thus, a language C is weakly $\leq_m^P$-complete for E if $C \in \mathrm{E}$ and *more than a negligible set* of the languages in E are $\leq_m^P$-reducible to C. This condition apparently generalizes the condition that C is $\leq_m^P$-complete for E, since the latter condition means that $C \in E$ and *all* the languages in E are $\leq_m^P$-reducible to C. (A similar remark applies to E_2.)

Juedes and Lutz [7] proved that every language C that is weakly complete for E or E_2 is strongly intractable, in the sense that it has a dense exponential complexity core. (Roughly speaking, this is a large set of very hard instances of the decision problem C.) Recently, Lutz [11] proved the existence of problems that are weakly $\leq_m^P$-complete, but not $\leq_m^P$-complete, for E. Thus, weakly $\leq_m^P$-complete problems for E are provably strongly intractable and need not be $\leq_m^P$-complete for E.

The purpose of the present note is to compare the notions of weak $\leq_m^P$-completeness for E and E_2. It is well-known that a language C is $\leq_m^P$-complete for E if and only if $C \in \mathrm{E}$ and C is $\leq_m^P$-complete for E_2. (This is because E_2 is the downward closure of E under $\leq_m^P$-reducibility.) Our Main Theorem (Theorem 4.4) shows that the situation is very different for weak $\leq_m^P$-completeness. Specifically, the Main Theorem establishes the following two facts.

(i) Every language that is weakly $\leq_m^P$-complete for E is weakly $\leq_m^P$-complete for E_2.

(ii) There is a language in E that is weakly $\leq_m^P$-complete for E_2, but not for E.

The proof of (i) makes essential use of a method developed by Ambos-Spies et al. [1] and stated as the Martingale Dilation Lemma in Section 3. The proof of (ii) makes essential use of intrinsic pseudorandomness [9, 13], the non-scarcity of weakly $\leq_m^P$-complete problems [1, 5, 6], and the Small Span Theorem [7]. (These things are all reviewed in Sections 3 and 4)

Fact (ii) asserts the existence of a language $C \in \mathrm{E}$ that is *not* weakly $\leq_m^P$-complete for E, but *is* weakly $\leq_m^P$-complete for the larger class E_2. This means that only a negligible set of languages in E are $\leq_m^P$-reducible to C, while a nonnegligible set of the languages in $\mathrm{E}_2 - \mathrm{E}$ are $\leq_m^P$-reducible to C.

2. Preliminaries

In this note, $[\![\psi]\!]$ denotes the *Boolean value* of the condition ψ, i.e.,

$$[\![\psi]\!] = \begin{cases} 1 & \text{if } \psi, \\ 0 & \text{if not } \psi. \end{cases}$$

All *languages* here are sets of binary strings, i.e., sets $A \subseteq \{0,1\}^*$. We identify each language A with its *characteristic sequencer* $\chi_A \in \{0,1\}^\infty$ defined by

$$\chi_A = [\![s_0 \in A]\!]\,[\![s_1 \in A]\!]\,[\![s_2 \in A]\!] \ldots,$$

where $s_0 = \lambda$, $s_1 = 0$, $s_2 = 1$, $s_3 = 00, \ldots$ is the standard enumeration of $\{0,1\}^*$. For $n \in \mathbb{N}$, we write $\chi_A[0..n-1]$ for the string consisting of the first n bits of χ_A. We write X^c for the complement of a set X of languages.

The *lower* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-span* of a language $A \subseteq \{0,1\}^*$ is

$$\mathrm{P_m}(A) = \{B \subseteq \{0,1\}^* \mid B \leq^{\mathrm{P}}_{\mathrm{m}} A\}.$$

The *upper* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-span* of A is

$$\mathrm{P_m^{-1}}(A) = \{B \subseteq \{0,1\}^* \mid A \leq^{\mathrm{P}}_{\mathrm{m}} B\}.$$

Note that if $A \equiv^{\mathrm{P}}_{\mathrm{m}} A'$ (i.e., if $A \leq^{\mathrm{P}}_{\mathrm{m}} A'$ and $A' \leq^{\mathrm{P}}_{\mathrm{m}} A$), then $\mathrm{P_m}(A) = \mathrm{P_m}(A')$ and $\mathrm{P_m^{-1}}(A) = \mathrm{P_m^{-1}}(A')$. The *lower* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-span* of a set X of languages is

$$\mathrm{P_m}(X) = \bigcup_{A \in X} \mathrm{P_m}(A).$$

3. Feasible martingales

Here we develop those aspects of feasible martingales, resource-bounded measure, and intrinsic pseudorandomness that are needed for our Main Theorem. For more details, motivation, and examples, the reader is referred to any of the papers [7, 9–13].

Martingales were used extensively by Schnorr [16–19] in his investigation of random and pseudorandom sequences. More recently, Lutz [9–12] has used martingales as a means of developing measure in complexity classes.

Definition.

1. A *martingale* is a function $d : \{0,1\}^* \to [0,\infty)$ satisfying the condition

$$d(w) = \frac{d(w0) + d(w1)}{2} \qquad (*)$$

   for all $w \in \{0,1\}^*$.

2. Let $t : \mathbb{N} \to \mathbb{N}$. A martingale d is a $t(n)$*-martingale* if there is a function $\hat{d} : \mathbb{N} \times \{0,1\}^* \to \mathbb{Q}$ with the following two properties.
   (a) There is an algorithm that, for all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$, computes $\hat{d}(r,w)$ in $O(t(r + |w|))$ steps.
   (b) For all $r \in \mathbb{N}$ and $w \in \{0,1\}^*$,

$$|\hat{d}(r,w) - d(w)| \leq 2^{-r}.$$

3. Let $t : \mathbb{N} \to \mathbb{N}$. A martingale d is an *exact* $t(n)$*-martingale* if d has nonnegative rational values (i.e., $d : \{0,1\}^* \to \mathbb{Q} \cap [0,\infty)$) and there is an algorithm that, for all $w \in \{0,1\}^*$, computes $d(w)$ in $O(t(|w|))$ steps.

4. A martingale d *succeeds* on a language $A \subseteq \{0,1\}^*$, and we write $A \in S^\infty[d]$, if

$$\limsup_{n\to\infty} d(\chi_A[0..n-1]) = \infty.$$

Intuitively, a martingale d is a betting strategy that, given a language A, starts with capital (amount of money) $d(\lambda)$ and bets on the membership or nonmembership of the successive strings $s_0, s_1, s_2, \ldots$ (the standard enumeration of $\{0,1\}^*$) in A. Prior to betting on a string s_n, the strategy has capital $d(w)$, where

$$w = [\![s_0 \in A]\!] \cdots [\![s_{n-1} \in A]\!].$$

After betting on the string s_n, the strategy has capital $d(wb)$, where $b = [\![s_n \in A]\!]$. Condition (∗) ensures that the betting is fair. The strategy succeeds on A if its capital is unbounded as the betting progresses.

The following lemma shows that $t(n)$-martingales can be replaced by exact martingales with a relatively small increase in computig time. This result has also been proven independently by Mayordomo [14].

Lemma 3.1 (Exact Computation Lemma). *Let $t: \mathbb{N} \to \mathbb{N}$ be nondecreasing with $t(n) \geq n$. Then, for every $t(n)$-martingale d, there is an exact $n \cdot t(2n+2)$-martingale $\tilde{d}$ such that $S^\infty[d] \subseteq S^\infty[\tilde{d}]$.*

Proof. Assume the hypothesis. Fix d and $\hat{d}$ such that $\hat{d}$ testifies that d is a $t(n)$-martingale. Define functions $d_1, d_2, \tilde{d}: \{0,1\}^* \to \mathbb{Q}$ by

$$d_1(w) = \hat{d}(|w| + 2, w),$$

$$d_2(w) = d_1(w) + 2^{-|w|},$$

$$\tilde{d}(\lambda) = d_2(\lambda),$$

$$\tilde{d}(w0) = \tilde{d}(w) - d_2(w) + d_2(w0),$$

$$\tilde{d}(w1) = \tilde{d}(w) + d_2(w) - d_2(w0).$$

It is routine to verify that the following conditions hold for all $w \in \{0,1\}^*$.

(i) $|d_1(w) - [d_1(w0) + d_1(w1)]/2| < 2^{-(|w|+1)}$.

(ii) $d_2(w) > [d_2(w0) + d_2(w1)]/2$.

(iii) $\tilde{d}(w) \geq d_2(w) > d(w)$.

By (iii) and inspection, $\tilde{d}$ is an exact $n \cdot t(2n+2)$-martingale satisfying $S^\infty[d] \subseteq S^\infty[\tilde{d}]$. □

We next explain a useful technique that was developed very recently by Ambos-Spies et al. [1].

Definition. The *restriction* of a string $w \in \{0,1\}^*$ to a language $A \subseteq \{0,1\}^*$ is the string $w \upharpoonright A$ defined by the following recursion.

(i) $\lambda \upharpoonright A = \lambda$.

(ii) For $w \in \{0,1\}^*$ and $b \in \{0,1\}$,

$$(wb)\upharpoonright A = \begin{cases} (w\upharpoonright A)b & \text{if } s_{|w|} \in A, \\ w\upharpoonright A & \text{if } s_{|w|} \notin A. \end{cases}$$

(That is, $w\upharpoonright A$ is the concatenation of the successive bits $w[i]$ for which $s_i \in A$.)

Definition. A function $f:\{0,1\}^* \to \{0,1\}^*$ is *strictly increasing* if, for all $x, y \in \{0,1\}^*$,

$$x < y \;\Rightarrow\; f(x) < f(y),$$

where $<$ is the standard ordering of $\{0,1\}^*$.

Notation. If $f:\{0,1\}^* \to \{0,1\}^*$, then for each $n \in \mathbb{N}$, let n_f be the unique integer such that $f(s_n) = s_{n_f}$.

Observation 3.2. If $f:\{0,1\}^* \to \{0,1\}^*$ is strictly increasing and $A \subseteq \{0,1\}^*$, then for all $n \in \mathbb{N}$,

$$\chi_{f^{-1}(A)}[0..n-1] = \chi_A[0..n_f - 1]\upharpoonright range(f).$$

Definition. If $f:\{0,1\}^* \to \{0,1\}^*$ is strictly increasing and d is a martingale, then the *f-dilation* of d is the function

$$f\hat{}d:\{0,1\}^* \to [0,\infty),$$

$$f\hat{}d(w) = d(w\upharpoonright range(f)).$$

Intuitively, the f-dilation of d is a strategy for betting on a language A, assuming that d itself is a good betting strategy for betting on the language $f^{-1}(A)$. Given an opportunity to bet on the membership or nonmembership of a string $y \in A$, $f\hat{}d$ refrains from betting unless $y = f(x)$, in which case $f\hat{}d$ bets exactly as d would bet on the membership or nonmembership of x in $f^{-1}(A)$.

The following lemma is implicit in the recent proof by Ambos-Spies et al. that every n^2-random language in E is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E.

Lemma 3.3. (Martingale Dilation Lemma – Ambos-Spies et al. [1]). *If $f:\{0,1\}^* \to \{0,1\}^*$ is strictly increasing and d is a martingale, then $f\hat{}d$ is also a martingale. Moreover, for every language $A \subseteq \{0,1\}^*$, if d succeeds on $f^{-1}(A)$, then $f\hat{}d$ succeeds on A.*

Proof. Assume the hypothesis. It is routine to check that $f\hat{}d$ is a martingale. Also, for all $A \subseteq \{0,1\}^*$ and $n \in \mathbb{N}$, Observation 3.2 tells us that

$$\begin{aligned} d(\chi_{f^{-1}(A)}[0..n-1]) &= d(\chi_A[0..n_f - 1]\upharpoonright range(f)) \\ &= f\hat{}d(\chi_A[0..n_f - 1]) \end{aligned}$$

Thus, if d succeeds on $f^{-1}(A)$, then

$$\limsup_{n\to\infty} f^{\wedge}d\,(\chi_A[0..n-1]) \geq \limsup_{n\to\infty} d(\chi_{f^{-1}(A)}[0..n-1]) = \infty,$$

so $f^{\wedge}d$ succeeds on A. □

We now use martingales to develop the basic ideas of measure in E and E_2.

Definition.
1. A martingale d is a *p-martingale* if there exists $k \in \mathbb{N}$ such that d is an n^k-martingale.
2. A martingale d is a p_2-*martingale* if there exists $k \in \mathbb{N}$ such that d is a $2^{(\log n)^k}$-martingale.

Thus a p-martingale is a martingale that is computable (to within 2^{-r}) in polynomial time, while a p_2-martingale is a martingale that is computable in quasi-polynomial time.

Definition (Lutz [9]).
1. A set X of languages has *p-measure* 0, and we write $\mu_p(X) = 0$, if there is a p-martingale d such that $X \subseteq S^\infty[d]$.
2. A set of languages has p_2-*measure* 0, and we write $\mu_{p_2}(X) = 0$, if there is a p_2-martingale d such that $X \subseteq S^\infty[d]$.

Definition (Lutz [9]).
1. A set X of languages has *measure* 0 *in* E, and we write $\mu(X \mid E) = 0$, if $\mu_p(X \cap E) = 0$.
2. A set X of languages has *measure* 0 *in* E_2, and we write $\mu(X \mid E_2) = 0$, if $\mu_{p_2}(X \cap E_2) = 0$.
3. A set X of languages has *measure* 1 *in* E, and we write $\mu(X \mid E) = 1$, if $\mu(X^c \mid E) = 0$. In this case, we say that X contains *almost every* element of E.
4. A set X of languages has *measure* 1 *in* E_2, and we write $\mu(X \mid E_2) = 1$, if $\mu(X^c \mid E_2) = 0$. In this case, we say that X contains *almost every* element of E_2.
5. The expression $\mu(X \mid E) \neq 0$ means that X does *not* have measure 0 in E. Note that this does *not* assert that "$\mu(X \mid E)$" has some nonzero value. Similarly, the expression $\mu(X \mid E_2) \neq 0$ means that X does not have measure 0 in E_2.

It is shown in [9] that these definitions endow E and E_2 with internal measure structure. This structure justifies the intuition that, if $\mu(X \mid E) = 0$, then $X \cap E$ is a *negligibly small* subset of E (and similarly for E_2). In particular, we have the following theorem.

Theorem 3.4 (Lutz [9]).
1. $\mu(E \mid E) \neq 0$.
2. $\mu(E_2 \mid E_2) \neq 0$.

We conclude this section with a very brief mention of intrinsic pseudo-randomness.

Definition (Lutz [9]). A language $A \subseteq \{0,1\}^*$ is *p-random*, and we write $A \in \mathrm{RAND}(\mathrm{p})$, if $\mu_{\mathrm{p}}(\{A\}) \neq 0$, i.e., if the singleton set $\{A\}$ does *not* have p-measure 0.

That is, A is p-random if there is no p-martingale that succeeds on A.

It is easy to see that $\mu_{\mathrm{p}}(\{A\}) = 0$ for all $A \in \mathrm{E}$, i.e., that no element of E is p-random [9]. However, the following result says that almost every element of E_2 is p-random.

Theorem 3.5 (Lutz [9, 13]). $\mu(\mathrm{RAND}(\mathrm{p}) | \mathrm{E}_2) = 1$.

4. Weak completeness

In this section we prove our Main Theorem, comparing weak $\leqslant_{\mathrm{m}}^{\mathrm{P}}$-completeness in E and E_2. We first define these terms precisely.

In standard terminology, a language C is $\leqslant_{\mathrm{m}}^{\mathrm{P}}$*-complete* for a complexioty class $\mathscr{C}$ if $C \in \mathscr{C} \subseteq \mathrm{P}_{\mathrm{m}}(C)$. The following definition generalizes this notion for the complexity classes E and E_2.

Definition.

1. A language C is *weakly* $\leqslant_{\mathrm{m}}^{\mathrm{P}}$*-complete* for E if $C \in \mathrm{E}$ and $\mu(\mathrm{P}_{\mathrm{m}}(C) | \mathrm{E}) \neq 0$.
2. A language C is *weakly* $\leqslant_{\mathrm{m}}^{\mathrm{P}}$*-complete* for E_2 if $C \in \mathrm{E}_2$ and $\mu(\mathrm{P}_{\mathrm{m}}(C) | \mathrm{E}_2) \neq 0$.

Notation.

$$\mathrm{C}_{\mathrm{E}} = \{C \mid C \text{ is } \leqslant_{\mathrm{m}}^{\mathrm{P}}\text{-complete for E}\}.$$

$$\mathrm{C}_{\mathrm{E}_2} = \{C \mid C \text{ is } \leqslant_{\mathrm{m}}^{\mathrm{P}}\text{-complete for } \mathrm{E}_2\}.$$

$$\mathrm{WC}_{\mathrm{E}} = \{C \mid C \text{ is weakly } \leqslant_{\mathrm{m}}^{\mathrm{P}}\text{-complete for E}\}.$$

$$\mathrm{WC}_{\mathrm{E}_2} = \{C \mid C \text{ is weakly } \leqslant_{\mathrm{m}}^{\mathrm{P}}\text{-complete for } \mathrm{E}_2\}.$$

It is well-known that $\mathrm{E} \cap \mathrm{C}_{\mathrm{E}_2} = \mathrm{C}_{\mathrm{E}}$. (This is clear because $\mathrm{E}_2 = \mathrm{P}_{\mathrm{m}}(\mathrm{E})$.) Theorem 3.4 implies that $\mathrm{C}_{\mathrm{E}} \subseteq \mathrm{WC}_{\mathrm{E}}$, and Lutz [11] has proven that $\mathrm{C}_{\mathrm{E}} \neq \mathrm{WC}_{\mathrm{E}}$. We thus have

$$\mathrm{E} \cap \mathrm{C}_{\mathrm{E}_2} = \mathrm{C}_{\mathrm{E}} \subsetneqq \mathrm{WC}_{\mathrm{E}}.$$

Our objective in the present note is to compare the classes WC_{E} and $\mathrm{E} \cap \mathrm{WC}_{\mathrm{E}_2}$. We first mention two known results that are used in our argument.

Theorem 4.1 (Small Span Theorem – Juedes and Lutz [7]). *For every* $A \in \mathrm{E}$,

$$\mu(\mathrm{P}_{\mathrm{m}}(A) | \mathrm{E}) = 0$$

or

$$\mu_{\mathrm{P}}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(A)|\mathrm{E}) = 0.$$

Theorem 4.2 (Juedes [5,6], Ambos-Spies et al. [1]). $\mu(\mathrm{WC}_{\mathrm{E}_2}|\mathrm{E}_2) \neq 0$.

Remark. Juedes [5,6] proved Theorem 4.2 by a refinement of the martingale diagonalization method of Lutz [11]. Very recently, and independently of [5,6], Ambos-Spies et al. [1] used a different argument to obtain the result $\mu(\mathrm{WC}_{\mathrm{E}}|\mathrm{E}) = 1$. A routine modification of their argument gives the result $\mu(\mathrm{WC}_{\mathrm{E}_2}|\mathrm{E}_2) = 1$, which is stronger than Theorem 4.2.

We also use the following very general lemma.

Lemma 4.3. *Let X be any set of languages. If $\mu(\mathrm{P}_{\mathrm{m}}(X)|\mathrm{E}_2) = 0$, then $\mu(X|\mathrm{E}) = 0$.*

Proof. Assume that $\mu(\mathrm{P}_{\mathrm{m}}(X)|\mathrm{E}_2) = 0$. Then there is a p_2-martingale d such that $\mathrm{P}_{\mathrm{m}}(X) \cap \mathrm{E}_2 \subseteq S^\infty[d]$. Fix $k \geqslant 1$ such that d is a $2^{(\log n)^k}$-martingale. By the exact computation lemma, there is an exact $2^{(\log n)^{k+1}}$-martingale $\tilde{d}$ such that $S^\infty[d] \subseteq S^\infty[\tilde{d}]$. Define

$$f: \{0,1\}^* \to \{0,1\}^*$$

$$f(x) = 0^{|x|^{k+1}} 1x.$$

Note that f is strictly increasing, so $f\hat{}\tilde{d}$, the f-dilation of $\tilde{d}$, is a martingale. The time required to compute $f\hat{}\tilde{d}(w)$ is

$$\mathrm{O}(|w|^2 + 2^{(\log|w'|)^{k+1}})$$

steps, where $w' = w\restriction range(f)$. (This allows $\mathrm{O}(|w|^2)$ steps to compute w' and then $\mathrm{O}(2^{(\log|w'|)^{k+1}})$ steps to compute $\tilde{d}(w')$.) Now $|w'|$ is bounded above by the number of strings x such that $|x|^{k+1} + |x| + 1 \leqslant |s_{|w|}| = \lfloor \log(1+|w|) \rfloor$, so

$$|w'| \leqslant 2^{1+(\log(1+|w|))^{1/(k+1)}}.$$

Putting these things together, the time required to compute $f\hat{}\tilde{d}(w)$ is

$$\mathrm{O}(|w|^2 + 2^{(1+(\log(1+|w|))^{1/(k+1)})^{k+1}}) = \mathrm{O}(|w|^2)$$

steps. Thus $f\hat{}\tilde{d}$ is an n^2-martingale.

Now let $A \in X \cap \mathrm{E}$. Then $f^{-1}(A) \in \mathrm{P}_{\mathrm{m}}(A) \cap \mathrm{E}_2 \subseteq S^\infty[d] \subseteq S^\infty[\tilde{d}]$, so $A \in S^\infty[f\hat{}\tilde{d}]$, by the Martingale Dilation Lemma. This shows that $X \cap \mathrm{E} \subseteq S^\infty[f\hat{}\tilde{d}]$. Since $f\hat{}\tilde{d}$ is an n^2-martingale, it follows that $\mu(X|\mathrm{E}) = \mu_{\mathrm{P}}(X \cap \mathrm{E}) = 0$. $\square$

Note that Lemma 4.3 implies that, if X is a set of languages that is closed under $\leqslant_{\mathrm{m}}^{\mathrm{P}}$-reductions, then $\mu(X|\mathrm{E}) = 0$ if and only if $\mu(X|\mathrm{E}_2) = 0$.

We now have enough machinery to give an easy proof of our main result.

Theorem 4.4 (Main Theorem). $\mathrm{WC_E} \subsetneq \mathrm{E} \cap \mathrm{WC_{E_2}}$.

Proof. It is clear that $\mathrm{WC_E} \subseteq \mathrm{E}$. To see that $\mathrm{WC_E} \subseteq \mathrm{WC_{E_2}}$, let $C \in WC_{\mathrm{E}}$. Then $\mu(\mathrm{P_m}(C)|\mathrm{E}) \neq 0$, so Lemma 4.3 with $X = \mathrm{P_m}(C)$ tells us that $\mu(\mathrm{P_m}(C)|\mathrm{E_2}) = \mu(\mathrm{P_m}(\mathrm{P_m}(C))|\mathrm{E_2}) \neq 0$. Thus $C \in \mathrm{WC_{E_2}}$, completing the proof that $\mathrm{WC_E} \subseteq \mathrm{E} \cap \mathrm{WC_{E_2}}$.

To see that $\mathrm{E} \cap \mathrm{WC_{E_2}} \not\subseteq \mathrm{WC_E}$, fix $C \in \mathrm{RAND(p)} \cap \mathrm{WC_{E_2}}$. (Such a language C exists by Theorems 3.5 and 4.2.) Fix $k \geq 1$ such that $C \in \mathrm{DTIME}(2^{n^k})$ and let

$$C' = \{0^{|x|^k} 1x \mid x \in C\}.$$

Note that $C' \in \mathrm{E}$ and $C' \equiv_m^{\mathrm{P}} C$, whence $C' \in \mathrm{E} \cap \mathrm{WC_{E_2}}$.

Since $C \in \mathrm{P_m^{-1}}(C') \cap \mathrm{RAND(p)}$, we have $\mu_{\mathrm{p}}(\mathrm{P_m^{-1}}(C')) \neq 0$. Since $C' \in \mathrm{E}$, it follows by the Small Span Theorem that $\mu(\mathrm{P_m}(C')|\mathrm{E}) = 0$. Thus $C' \notin \mathrm{WC_E}$, completing the proof that $\mathrm{E} \cap \mathrm{WC_{E_2}} \not\subseteq \mathrm{WC_E}$. $\square$

Putting the Main Theorem together with previously known results, we have

$$\mathrm{E} \cap \mathrm{C_{E_2}} = \mathrm{C_E} \subsetneq \mathrm{WC_E} \subsetneq \mathrm{E} \cap \mathrm{WC_{E_2}}.$$

Acknowledgements

The second author thanks Klaus Ambos-Spies, Harry Buhrman, Steve Fenner, Elvira Mayordomo and Zheng Xizhong for fun and helpful discussions during the February, 1994 Structure and Complexity Seminar at Schloss Dagstuhl.

References

[1] K. Ambos-Spies, S.A. Terwijn and Zheng Xizhong, Resource bounded randomness and weakly complete problems, *Proc. Fifth Ann. Internat. Symp. on Algorithms and Computation* (Springer, Berlin, 1994) 369–377.

[2] J.L. Balcázar and U. Schöning, Bi-immune sets for complexity classes, *Math. Systems Theory* **18** (1985) 1–10.

[3] J. Hartmanis and R.E. Stearns, On the computational omplexity of algorithms, *Trans. Amer. Math. Soc.* **117** (1965) 285–306.

[4] D.T. Huynh, Some observations about the randomness of hard problems, *SIAM J. Comput.* **15** (1986) 1101–1105.

[5] D.W. Juedes, The complexity and distribution of computationally useful problem, Ph.D. Thesis, Iowa State University, 1994.

[6] D.W. Juedes, Weakly complete problems are not rare, submitted.

[7] D.W. Juedes and J.H. Lutz, The complexity and distribution of hard problems, *SIAM J. Comput.* **24** (1995) to appear. Also in *Proc. 34th IEEE Symp. on Foundations of Computer Science*, Palo Alto, CA (IEEE Computer Society Press, Silver Spring, MD, 1993) 177–185.

[8] K. Ko, P. Orponen, U. Schöning and O. Watanabe, Instance complexity, *J. ACM* **41** (1994) 96–121.

[9] J.H. Lutz, Almost everywhere high nonuniform complexity, *J. Comput. System Sci.* **44** (1992) 220–258.

[10] J.H. Lutz, The quantitative structure of exponential time, *Proc. Eighth Structure in Complexity Theory Conference* (IEEE Computer Society Press, Silver Spring, MD, 1993) 158–175.

[11] J.H. Lutz, Weakly hard problems, *SIAM J. Comput.*, to appear. See also *Proc. Ninth Structure in Complexity Theory Conference* (IEEE Computer Society Press, Silver Spring, MD, 1994) 146-161.
[12] J.H. Lutz, Resource-bounded measure, in preparation.
[13] J.H. Lutz, Intrinsically pseudorandom sequences, in preparation.
[14] E. Mayordomo, Contribuions to the study of resource-bounded measure, Ph.D. Thesis, Universitat Politècnica de Catalunya, 1994.
[15] P. Orponen and U. Schöning, The density and complexity of polynomial cores for intractable sets, *Inform. Control* **70** (1986) 54-68.
[16] C.P. Schnorr, Klassifikation der Zufallsgesetze nach Komplexität und Ordnung, *Z. Wahrscheinlichkeitstheorie verw. Geb.* **16** (1970) 1-21.
[17] C.P. Schnorr, A unified approach to the definition of random sequences, *Math. Systems Theory* **5** (1971) 246-258.
[18] C.P. Schnorr, Zufälligkeit und Wahrscheinlichkeit, Lecture Notes in Mathematics, Vol. 218 (Springer, Berlin, 1971).
[19] C.P. Schnorr, Process complexity and effective random tests, *J. Comput. System Sci.* **7** (1973) 376-388.
[20] U. Schöning, Complete sets and closeness to complexity classes, *Math. Systems Theory* **19** (1986) 29-41.